Primos e Divisores Espertos

Rafael Amiune

1 Introdução

No curso de Teoria dos Números do NOIC, você já conheceu as propriedades básicas dos inteiros, seus divisores e, em especial, dos números primos. Neste material, vamos avançar um pouco mais: veremos como explorar essas propriedades, além de aprender novas técnicas, para resolver uma grande variedade de problemas de Teoria dos Números.

Em olimpíadas de matemática, é bastante comum surgirem problemas cuja solução depende de escolher um número primo com uma característica especial — um "primo esperto". Muitas vezes, identificar esse primo já fornece informações decisivas ou até resolve o problema por completo. Por isso, é fundamental saber como procurar (e reconhecer) esses primos.

O material está dividido em três seções, cada uma dedicada a uma ideia central, acompanhada de exemplos, aplicações em problemas típicos de olimpíada e, ao final, uma lista de exercícios. Apresentamos a solução de alguns problemas de cada tópico com o intuito de prepará-lo(a) para resolver os exercícios propostos, entre outros. Por isso, é crucial que tente resolver tanto os exercícios da lista quanto os problemas resolvidos no texto antes de consultar as soluções. Aproveite!

2 Resolvendo Problemas

2.1 Construindo Divisores

Para começar essa seção, vamos para um problema motivador, do teste de seleção brasileiro para a Olimpíada de Matemática do Cone Sul de 2021.

(Cone Sul TST 2021) Sejam a, b, c inteiros positivos. Prove que existe um inteiro não negativo k tal que

$$\text{mdc}(a^k + bc, b^k + ca, c^k + ab) > 1.$$

Note que o problema é análogo a encontrar um k tal que um mesmo primo divida as três parcelas do mdc. Vamos supor que exista tal primo p. Em particular,

$$a^k + bc \equiv 0 \pmod{p} \implies a^{k+1} \equiv -abc \pmod{p}$$

Analogamente, obtemos $a^{k+1} \equiv b^{k+1} \equiv c^{k+1} \pmod{p}$. Uma conjectura razoável, seria que $k = p-2$ é uma boa escolha, pois, para um $p \nmid a, b, c$, sabemos que $a^{p-1} \equiv b^{p-1} \equiv c^{p-1} \equiv 1 \pmod{p}$. Então gostaríamos que $-abc \equiv 1 \pmod{p}$, porém basta tomar $p \mid abc + 1$! A seguir está a solução escrita da maneira adequada para uma prova.

Solução: Considere um primo $p \mid abc + 1$. Afirmamos que

$$p \mid \text{mdc}(a^{p-2} + bc, b^{p-2} + ca, c^{p-2} + ab).$$

Isso claramente terminaria o problema, com a escolha de $k = p - 2$. De fato,

$$a^{p-2} + bc \equiv a^{p-2} - a^{-1} \equiv a^{-1}(a^{p-1} - 1) \equiv 0 \pmod{p}$$

Analogamente para as outras parcelas, obtemos o resultado desejado. □

A ideia abordada nesta seção é, de fato, bastante simples. Como se pode observar, utilizamos apenas o **Pequeno Teorema de Fermat**, aliado a manipulações usuais de congruências, em nossa solução. Para consolidar o domínio desse tipo de problema, a prática é indispensável. Por isso, apresentaremos a seguir apenas mais um problema, que exemplifica a aplicação dessa técnica em um problema envolvendo sequências, para que, posteriormente, você possa partir para a lista de exercícios. A solução do problema que iremos apresentar é muito semelhante à do problema anterior, então é crucial que tente resolvê-lo antes de ler a sua solução.

(Cone Sul TST 2025) Sejam $m \geq 2$ um inteiro positivo e $p \geq 5$ um número primo. Considere a sequência $a_1, a_2, \ldots$ definida por $a_n = (p-2)^n + p^n - m$, para $n \geq 1$. Seja q o menor primo tal que existe um termo da sequência que é múltiplo de q. Determine todos os pares (m,p) para os quais $q \geq m$.

Inicialmente, é natural procurar por primos que dividem algum dos termos da sequência. Em particular, para m par temos $a_1 = 2p - 2 - m$, que é par, ou seja, $q = 2$, que implica $m = 2$. Podemos supor m ímpar. Nesse caso, os n nos expoentes nos induzem a considerar $n = t - 1$, com t primo, pelo **Pequeno Teorema de Fermat**. Caso não o tenha feito, tente terminar o problema a partir dessa ideia que, embora simples aniquila o problema, de maneira semelhante

ao anterior. A seguir apresentamos a solução, de maneira adequada para uma competição.

Solução: Veja que $(2,p)$ é solução, uma vez que 2 divide todos os termos. Analogamente, $(3,p)$ é solução, pois 2 não divide nenhum termo, ou seja $q \geq 3$. Caso m seja par, temos $2 \mid a_1$, que implica $q = 2$, ou seja, $m = 2$. Agora suponhamos m ímpar maior do que 3.

Considere um primo $t \mid m-2$ tal que $t \neq p$. Afirmamos que $q \leq t$, um absurdo, pois $t < m$. Temos dois casos:

- $t \mid p-2 \rightsquigarrow a_t \equiv p^t + (p-2)^t - m \equiv 2^t - 2 \equiv 0 \pmod{t}$.
- $t \nmid p-2 \rightsquigarrow a_{t-1} \equiv p^{t-1} + (p-2)^{t-1} - m \equiv 1 + 1 - m \equiv 0 \pmod{t}$.

Agora, sabemos que o único divisor primo de $m-2$ é p, ou seja, $m = p^k + 2$. Neste caso, podemos considerar $a_k = (p-2)^k - 2 < m$. Caso $a_k > 1$, estamos feitos, mas $(p-2)^k - 2 \geq 3^k - 2$, que implica $k = 1$ e $p = 3$, ou seja, $(m,p) = (7,5)$, mas então $a_2 = 27 \Rightarrow q \leq 3 < m$. Portanto, as soluções são $(2,p)$ e $(3,p)$ para todos primo $p \geq 5$. □

2.2 *Menor Primo*

A estratégia de considerar um primo minimal é bastante comum e constitui uma aplicação clássica do **Princípio do Extremo** na Teoria dos Números. Começaremos com um problema motivador, novamente.

> **(OBM 2022)** Inicialmente um número está escrito no quadro. Então, a cada minuto, Esmeralda escolhe um divisor $d > 1$ do número n escrito na lousa, apaga n e escreve $n + d$. Se o número inicial é 2022, qual é o maior número composto que Esmeralda nunca poderá escrever no quadro?

Uma observação imediata é que todos os números pares a partir de 2022 podem ser escritos, de modo que precisamos nos preocupar apenas com os números ímpares. Suponha, então, que M seja um número composto ímpar, e seja $d > 1$ um divisor de M. Note que $M - d$ é par e, além disso, é múltiplo de d. Assim, se $M - d \geq 2022$, conseguimos escrever M no quadro. Logo, para que M seja um candidato ao número desejado, deve-se ter $M - d < 2022$ para todo divisor d de M.

Se nosso objetivo é obter uma cota superior para M, é natural considerar divisores d pequenos. É exatamente nesse ponto que o seguinte **Lema** se torna útil.

Lema: Se $n \in \mathbb{Z}_{>0}$ é um número composto e p é seu menor divisor primo, então vale que $p \leq \sqrt{n}$.

Prova: Suponha por absurdo que $p > \sqrt{n}$. Como n é composto, sabemos que $n = ab$, com $a, b > 1$. Porém, pela minimalidade de p, temos $a, b \geq p \implies n > \sqrt{n} \cdot \sqrt{n} \implies n > n$, Absurdo! □

Agora, vamos aplicar essa propriedade simples para finalizar a solução do problema!

Solução: Seja M o número desejado. Note que podemos escrever todos os números pares maiores que 2022 no quadro, logo M é ímpar. Seja d o menor divisor primo de M. Como M é ímpar, temos que $M - d$ é par, mas também temos que $d \mid M - d$, logo podemos escrever M a partir de $M - d$. Deste modo, $M - d < 2022$.

Pelo nosso **Lema**, sabemos que $d \leq \sqrt{M}$, então

$$M - \sqrt{M} - 2022 < 0 \implies \sqrt{M} < \frac{1 + \sqrt{8089}}{2} \implies M \leq 2067$$

Como $2 \mid 2022$, $3 \mid 2022$ e $5 \mid 2022 + 3$, podemos tirar todos os múltiplos de 2, 3 ou 5 da jogada, sobrando apenas os seguintes números:

$$2023, 2027, 2029, 2033, 2039, 2041, 2047, 2051, 2053, 2057, 2059, 2063$$

Vamos provar que a resposta é $\boxed{2033}$. Basta mostrarmos que é possível escrever os números listados entre 2039 e 2063 e que não é possível escrever 2033.

- Os números $2029, 2053$ e 2063 são primos, então não contam para a resposta.
- Para escrever 2041, basta fazer $2028 \rightsquigarrow 2028 + 13 = 2041$.
- Para escrever 2047, basta fazer $2024 \rightsquigarrow 2024 + 23 = 2047$.
- Para escrever 2051, basta fazer $2024 \rightsquigarrow 2044 + 7 = 2051$.
- Para escrever 2057, basta fazer $2046 \rightsquigarrow 2046 + 11 = 2057$.
- Para escrever 2059, basta fazer $2030 \rightsquigarrow 2030 + 29 = 2059$.

Como o menor divisor primo de 2033 é 19 e $2033 - 19 < 2022$, a resposta é, de fato, 2033. □

Embora tenhamos tomado o menor primo que divide um certo inteiro, as aplicações dessa ideia não se restringem a isso. Podemos tomar o menor divisor primo de uma certa sequência, por exemplo. Observe o seguinte problema:

(Folclore) Encontre todas as sequências finitas de inteiros positivos $a_1, a_2, \ldots, a_n$ tais que

$$a_1 \mid 2^{a_2} - 1, a_2 \mid 2^{a_3} - 1, \ldots, a_n \mid 2^{a_1} - 1.$$

Aqui, não temos muito controle sobre os termos da sequência; isto é, a princípio, eles podem assumir qualquer valor. Por isso, uma boa estratégia é considerar um primo p que divida algum dos termos, digamos a_i. A partir dessa hipótese, obtemos a seguinte relação:

$$2^{a_{i+1}} \equiv 1 \pmod{p}.$$

Utilizando noções básicas de ordem, concluímos que $\text{ord}_p 2 \mid a_{i+1}$. Como sabemos que $\text{ord}_p 2 \mid p - 1$, pelo **Pequeno Teorema de Fermat**, obtemos

$$\text{ord}_p 2 \mid \text{mdc}(a_{i+1}, p - 1).$$

Mas e se pudéssemos forçar esse mdc a ser 1? Isso nos forneceria

$$2 \equiv 1 \pmod{p} \implies p \mid 1 \implies \text{Absurdo!}$$

Logo a sequência não teria divisores primos p e a única opção seria $a_1 = a_2 = \cdots = a_n = 1$. Entretanto, perceba que se p é o divisor primo minimal que divide algum termo, todos os divisores primos de a_{i+1} serão maiores do que $p - 1$ e o mdc será 1! Vamos para a solução!

Solução: Seja p o menor primo que divide algum termo a_i da sequência. Note que p deve ser maior do que 2, pois todos os termos da sequência dividem um número ímpar.

$$a_i \mid 2^{a_{i+1}} - 1 \implies 2^{a_{i+1}} \equiv 1 \pmod{p} \implies \text{ord}_p 2 \mid a_{i+1}$$

Porém, sabemos que $\text{ord}_p 2 \mid p - 1$, pelo **Pequeno Teorema de Fermat** (Em que $\text{ord}_p 2$ denota a ordem de 2 módulo p), logo $\text{ord}_p 2 \mid \text{mdc}(a_{i+1}, p - 1)$. Mas, todos os divisores primos de a_{i+1} são no mínimo p, ou seja, $\text{mdc}(a_{i+1}, p - 1) = 1 \implies \text{ord}_p 2 \mid 1 \implies \text{ord}_p 2 = 1 \implies p \mid 2^1 - 1 = 1 \implies$ Absurdo!

Portanto, não podemos tomar um divisor primo mínimo da sequência, isto é, nenhum termo tem um divisor primo. Então $a_1 = a_2 = \cdots = a_n = 1$, que funciona. □

2.3 *Primos com Restos Espertos*

Como último assunto do material, abordaremos o resto dos números primos na divisão por outros inteiros. O resto dos números em relação a um módulo é frequentemente crucial na resolução de problemas, e, por isso, encontrar um divisor primo com um resto estratégico pode ser muito útil. Em particular, primos da forma $p = 4k + 3$ têm propriedades bastante especiais, como ilustram os resultados a seguir.

Lema: Se $n \equiv 3 \pmod 4$, então existe $p \mid n$ primo com $p \equiv 3 \pmod 4$.

Prova: Suponha por absurdo que tal p não existe. Pelo **Teorema Fundamental da Aritmética**, sabemos que n pode ser fatorado como um produto de primos, porém, como n é ímpar, todos esses primos teriam que deixar resto 1 por 4, contrariando o fato de n deixar resto 3, absurdo! □

(Teorema Natalino de Fermat) Se a, b são inteiros e $p \equiv 3 \pmod 4$ um primo tal que $p \mid a^2 + b^2$, então $p \mid a$ e $p \mid b$.

Prova: Suponha por absurdo que p não divide a ou b, uma vez que se dividisse um deles teria que dividir o outro. Então temos:

$$a^2 \equiv -b^2 \pmod p \implies a^{p-1} \equiv (-1)^{\frac{p-1}{2}} \cdot b^{p-1} \equiv -b^{p-1} \pmod p$$

Porém, sabemos que $a^{p-1} \equiv b^{p-1} \equiv 1 \pmod p$ pelo **Pequeno Teorema de Fermat**, logo obtemos $1 \equiv -1 \pmod p \implies p \mid 2$, absurdo! □

Para ilustrar o poder desses resultados, vamos resolver um problema da OMCPLP de 2020 (Olimpíada de Matemática da Comunidade dos Países de Língua Portuguesa).

(OMCPLP 2020) Prove que não existem inteiros x e y, com $3 \nmid y$, tais que:

$$y^2 = x^3 - 2017$$

Sem nunca ter visto os lemas previamente demonstrados, esse problema pode se provar bem desafiador. Contudo, tendo em mente que podemos controlar muito bem coisas da forma $a^2 + b^2$, é natural tentar forçar essa estrutura a aparecer. Testanto alguns valores, pode se perceber uma "quase" solução para a nossa equação. Na verdade,

$$45^2 = 2^3 + 2017 \implies y^2 + 45^2 = x^3 + 2^3.$$

Agora, é natural procurar por um primo $p \equiv 3 \pmod 4$ que divida algum dos lados da equação. Observando a equação original, concluímos facilmente que $x \equiv 1 \pmod 4$. Além disso, temos

$$x^3 + 2^3 = (x+2)(x^2 - 2x + 4).$$

Portanto, $x + 2 \mid y^2 + 45^2$. Assim, pelo **Lema** previamente demonstrado, existe um primo $p \equiv 3 \pmod 4$ que divide $y^2 + 45^2$. No entanto, pelo **Teorema Natalino de Fermat**, tal primo deve dividir simultaneamente y e 45. A única possibilidade é $p = 3$, o que implica $3 \mid y$.

Solução: Observe que $45^2 - 2^3 = 2017$, portanto podemos trocar a igualdade desejada por:

$$y^2 + 45^2 = x^3 + 2^3$$

Entretanto,

$$x^3 \equiv y^2 + 2017 \equiv y^2 + 1 \pmod 4.$$

Como o lado direito pode assumir apenas os restos 1 ou 2, e x^3 nunca é congruente a $2 \pmod 4$, concluímos que $x \equiv 1 \pmod 4$. Além disso, o lado direito

$$x^3 + 2^3 = (x+2)(x^2 - 2x + 4)$$

fatora de modo que $x + 2 \equiv 3 \pmod 4$. Assim, pelo **Lema** anteriormente demonstrado, o lado direito deve possuir um divisor primo $p \equiv 3 \pmod 4$. Logo,

$$p \mid y^2 + 45^2 \implies p \mid 45 \implies p = 3 \implies 3 \mid y.$$

□

(Utilizamos o **Teorema Natalino de Fermat** na última passagem.)

Como mostrado por este belo problema, as propriedades dos primos da forma $4k + 3$ são muito poderosas. No entanto, também são bem interessantes os primos da forma $p = 3k + 2$, que eventualmente aparecem e são importantes de se ter em mente. Observe o seguinte resultado:

Lema: Sejam a, b são inteiros e $p = 3k+2$ um primo tal que $p \mid a^3 + b^3$, então $p \mid a + b$.

Prova: Se $p \mid a$ ou $p \mid b$ o resultado segue facilmente, então suponha que $p \nmid ab$. Nesse caso, temos

$$a^3 \equiv -b^3 \pmod{p} \implies a^{p+1} \equiv (-1)^{\frac{p+1}{3}} \cdot b^{p+1} \equiv b^{p+1} \pmod{p}$$

Entretanto, sabemos que $n^{p+1} \equiv n^2 \pmod{p}$, pelo **Pequeno Teorema de Fermat**, logo $a^2 \equiv b^2 \pmod{p} \implies a \equiv -b \pmod{p} \implies p \mid a+b$, sendo que o último passo se dá pela congruência original. □

O seguinte problema, da Shortlist da IMO, é um ótimo exemplo de uma aplicação desse lema.

(IMO Shortlist 2012) Encontre todas as triplas (x, y, z) de inteiros positivos tais que $x \leq y \leq z$ e

$$x^3(y^3 + z^3) = 2012(xyz + 2).$$

Solução: Primeiro vamos provar que $x \in \{1, 2\}$. Suponha por absurdo que algum primo $p > 2$ divide x. Então a quantidade de fatores p no lado esquerdo da equação é no mínimo 3, por causa do x^3, entretanto, $p \nmid xyz + 2$, pois $p \nmid 2$, então a quantidade de fatores p no lado direito é a quantidade de fatores p em 2012, que é $2^2 \cdot 503$, absurdo! Agora, temos duas opções:

$$y^3 + z^3 = 2012(yz + 2) \tag{1}$$
$$y^3 + z^3 = 503(yz + 1) \tag{2}$$

Note que, em ambos os casos, $503 \mid y^3 + z^3$, logo, pelo **Lema**, $503 \mid y + z$. Então podemos fazer a substituição $y + z = 503k$, obtendo as seguintes equações:

$$k(y^2 - yz + z^2) = 4yz + 8 \tag{3}$$
$$k(y^2 - yz + z^2) = yz + 1 \tag{4}$$

Se $k > 1$, a equação (4) implicaria

$$yz+1 \geq 2(y^2-yz+z^2) \implies 2(y-z)^2 \leq 1-yz \leq 0 \implies y=z \implies$$
$$\implies ky^2 = y^2+1 \implies y^2 = \frac{1}{k-1} \implies k=2 \implies y=1 \implies 503 \mid 2.$$

Que é um absurdo, logo a única opção para a equação (4) é $k=1$, que nos dá

$$(y-z)^2 = 1 \implies z = y+1 \implies \boxed{(x,y,z)=(2,251,252)}.$$

Agora, vamos olhar para a equação (3). Pela desigualdade das médias, sabemos que $y^2+z^2 \geq 2yz \implies y^2-yz+z^2 \geq yz$, então

$$4yz+8 \geq kyz \implies 8 \geq (k-4)yz$$

Porém, $y+z \geq 503 \implies z \geq 252 \implies yz \geq 252$. Portanto, se $k>4$ teríamos um absurdo, logo $k \leq 4$. Na equação original (1), temos y^3+z^3 par, logo $y+z$ é par, ou seja, k é par, que implica $k \in \{2,4\}$. Se $k=4$, então teríamos $y^2-yz+z^2 = yz+2 \implies (y-z)^2 = 2$, um absurdo. E se $k=2$, podemos escrever a equação como $(y+z)^2-5yz = 4 \implies 4 \cdot 503^2 - 5yz = 4$, que é um absurdo, pois $4 \cdot 503^2 - 4$ não é múltiplo de 5. Portanto a única solução é $\boxed{(x,y,z)=(2,251,252)}$. □

Para finalizar esta seção, vamos apresentar um teorema mais avançado, porém essencial quando o assunto é "primos com restos" e resolver um problema interessante logo em seguida.

(Teorema de Dirichlet) Sejam a, b inteiros positivos com $\text{mdc}(a,b)=1$. A progressão aritmética $x_n = an+b$ tem infinitos números primos.

A demonstração do Teorema de Dirichlet envolve ferramentas avançadas de teoria analítica dos números e ultrapassa o escopo deste material. Vamos ao problema!

Seja $f(x)$ um polinômio com coeficientes racionais. Prove que se $f(p)$ é primo pra todo p primo então $f(x)=x$ pra todo x ou $f(x)$ é constante igual a um número primo.

Solução: Caso $f(x)$ seja constante, claramente deve ser um número primo, logo assuma $f(x)$ não constante. Nesse caso, deve ser crescente, uma vez que

assume valores positivos pra x arbitrariamente grande. Se $f(p) = p$ pra infinitos valores de p então $f(x) = x$ pra todo x, logo, supondo por absurdo que $f(x) \neq x$ pra finitos valores de x, existe N tal que $f(p) \neq p$ pra todo $p > N$. Seja

$$f(x) = \frac{b_k}{c_k}x^k + \frac{b_{k-1}}{c_{k-1}}x^{k-1} + \cdots + \frac{b_0}{c_0}.$$

Como $f(x)$ é crescente, existe M tal que $f(x) > \max(b_0,\ldots,b_k,c_0,\ldots,c_k)$. Considere $p > \max(N,M)$, de modo que $f(p) = q \neq p$. Temos $f(p) \equiv 0 \pmod{q}$. Pelo **Teorema de Dirichlet**, existem infinitos primos $r > p$ tais que $r \equiv p \pmod{q}$. Para tal r, deve valer $f(r) \equiv f(p) \equiv 0 \pmod{q}$, donde $f(r) = q$, uma vez que é primo. Como vale pra infinitos valores de r, $f(x) = q$ pra todo x, absurdo! Logo $f(x) = x$ pra todo x, como queríamos. □

3 Lista de Exercícios

Aqui estão alguns problemas para você treinar! É importante destacar que eles não estão organizados por ordem de dificuldade. Boa prática e divirta-se!

Problema 1. (TM2 2024) Encontre todos os inteiros positivos a, b, c tais que $3ab = 2c^2$ e $a^3 + b^3 + c^3$ é duas vezes um número primo.

Problema 2. (IMO 2023) Determine todos os números inteiros $n > 1$ compostos que satisfazem a seguinte propriedade: se $d_1, d_2, \ldots, d_k$ são todos os divisores positivos de n com $1 = d_1 < d_2 < \cdots < d_k = n$, então d_i divide $d_{i+1} + d_{i+2}$ para todo $1 \leq i \leq k-2$.

Problema 3. (Cone Sul 2018) Defina o produto $P_n = 1! \cdot 2! \cdot 3! \cdots (n-1)! \cdot n!$.

a) Encontre todos os inteiros positivos m, tais que $\dfrac{P_{2020}}{m!}$ é um quadrado perfeito.

b) Prove que existem infinitos valores de n, tais que $\dfrac{P_n}{m!}$ é um quadrado perfeito para ao menos dois inteiros positivos m.

Problema 4. (EGMO 2025) Para um inteiro positivo N, sejam $c_1 < c_2 < \cdots < c_m$ todos os inteiros positivos menores do que N que são coprimos com N. Encontre todos os valores de $N \geq 3$ tais que

$$\text{mdc}(N, c_i + c_{i+1}) \neq 1$$

para todo $1 \leq i \leq m-1$.

Problema 5. (OBM 2024) Seja a_1 um inteiro positivo maior ou igual a 2. Considere a sequência tal que o seu primeiro termo é a_1, e para a_n, o n-ésimo termo da sequência, temos

$$a_{n+1} = \frac{a_n}{p_k^{e_k - 1}} + 1,$$

onde $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ é a fatoração em primos de a_n, com $1 < p_1 < p_2 < \cdots < p_k$, e $e_1, e_2, \ldots, e_k$ inteiros positivos. Determine para quais valores de a_1 a sequência é eventualmente periódica e quais são os possíveis períodos.

Problema 6. (OBM 2023) Para um inteiro positivo k, seja $p(k)$ o menor número primo que não divide k. Dado um inteiro positivo a, defina a sequência infinita $a_0, a_1, \ldots$ como $a_0 = a$ e, para $n > 0$, a_n é o menor inteiro positivo com as seguintes propriedades:

- a_n ainda não apareceu na sequência, isto é, $a_n \neq a_i$ para $0 \leq i < n$;
- $(a_{n-1})^{a_n} - 1$ é um múltiplo $p(a_{n-1})$.

Prove que todo inteiro positivo aparece na sequência.

Problema 7. (IMO 2024) Determine todos os pares de inteiros positivos (a, b) para os quais existem inteiros positivos g e N tais que

$$\text{mdc}(a^n + b, b^n + a) = g$$

para todos os inteiros positivos $n \geq N$.

Problema 8. (IMO 2025) Um divisor *noic* de um inteiro positivo N é um divisor positivo de N diferente do próprio N.
A sequência infinita $a_1, a_2, \ldots$ consiste de inteiros positivos, todos com ao menos três divisores *noic*. Para cada $n \geq 1$, o inteiro a_{n+1} é a soma dos três maiores divisores *noic* de a_n.
Determine todos os possíveis valores de a_1 para os quais a sequência é bem definida, ou seja, todo termo tem ao menos três divisores *noic*.

Problema 9. (Grécia 2025) Prove que não existem inteiros (x, y) tais que

$$x^3 = y^2 + 108.$$

Problema 10. (USA TST 2008) Seja n um inteiro. Prove que $n^7 + 7$ não é um quadrado perfeito.

Problema 11. (IMO 2008) Prove que existem infinitos inteiros positivos n tais que $n^2 + 1$ possui um divisor primo maior que $2n + \sqrt{2n}$.

4 Bibliografia

- https://artofproblemsolving.com/
- https://imo-official.org/
- Primos em Progressões Aritméticas (Ana Paula Chaves)